U.S. Marine Corps Forces, Pacific
Force Protection

Newsletter

3d Quarter CY21

Mission

To ensure that U.S. Marine Corps Forces operating within or transiting through, the U.S. Indo-Pacific Command (USINDOPACOM) Area of Responsibility (AOR) are prepared to survive, respond to, and recover from enemy threats, and natural hazards, in order to ensure freedom of action and continuity of operations.

From the Branch Head:

On September 1, 2021 the FP Branch sent out an all hands email containing MARADMIN 418/21 announcing September as National Insider Threat Awareness Month (NITAM). This email also contained the HQMC NITAM newsletter as well as the cultural awareness handout for information awareness. For requests for additional information, training, reporting, or questions in general, please contact the Force Protection Branch, and/or the Security Manager.

Hurricane season is upon us, and runs through 30 November. The National Weather Service has predicted 4 named storms, 3 hurricanes, and 2 major hurricanes will occur over the course of the 2021 hurricane season in the central Pacific. The Emergency Management section includes TCCOR actions and emergency planning for shelter-in-place scenarios. The Hawaii Emergency Management Agency recommends provisions/needs for a minimum of 14 days for each person in your household. Due to geographic dispersion, the safest course of action is to plan for 30 days.

Lastly, this quarter we would like to congratulate Mr. Brian Chun-Ming for his selection and promotion as the MARFORPAC Command Security Manager. We look forward to continued coordination between the Force Protection Branch and Command Security.

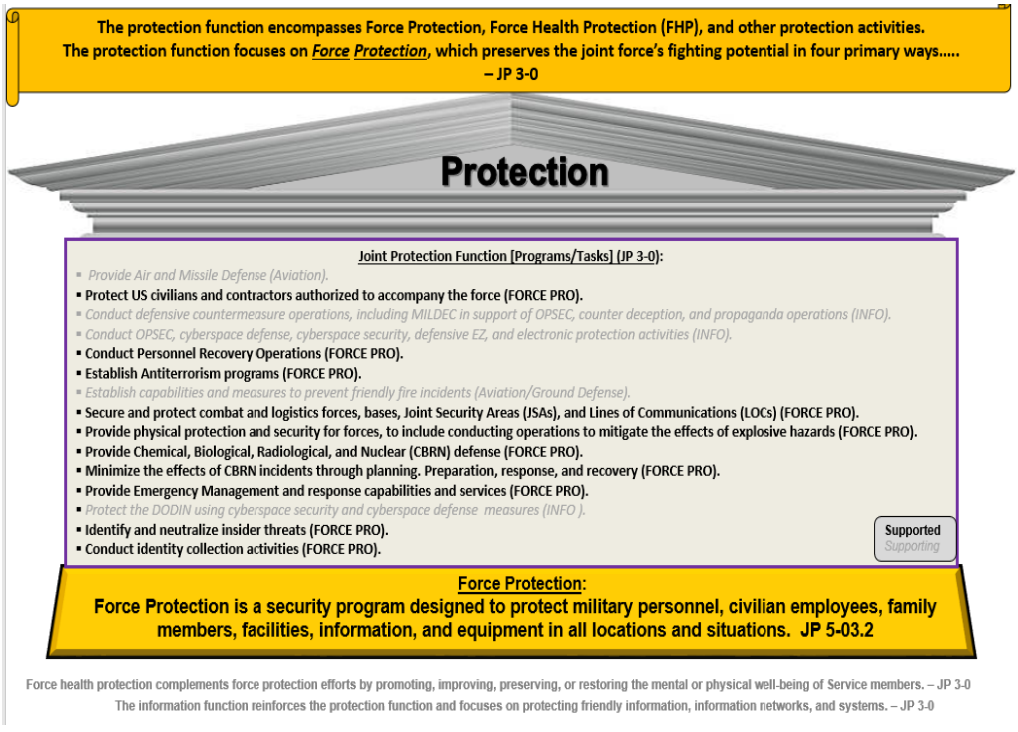


Table of Contents

Community Updates

MCDP-8, Marine Corps Protection
- New Publication
- **Currently out for FO/GO Review**
- OPR, DC PP&O, Security Division (PS)

MCWP 10-10, Marine Corps Protection
- New Publication.
- In Draft (OPR, USMC Protection Council)

Marine Corps Protection Policy
- New Publication
- In Draft (OPR, USMC Protection Council)

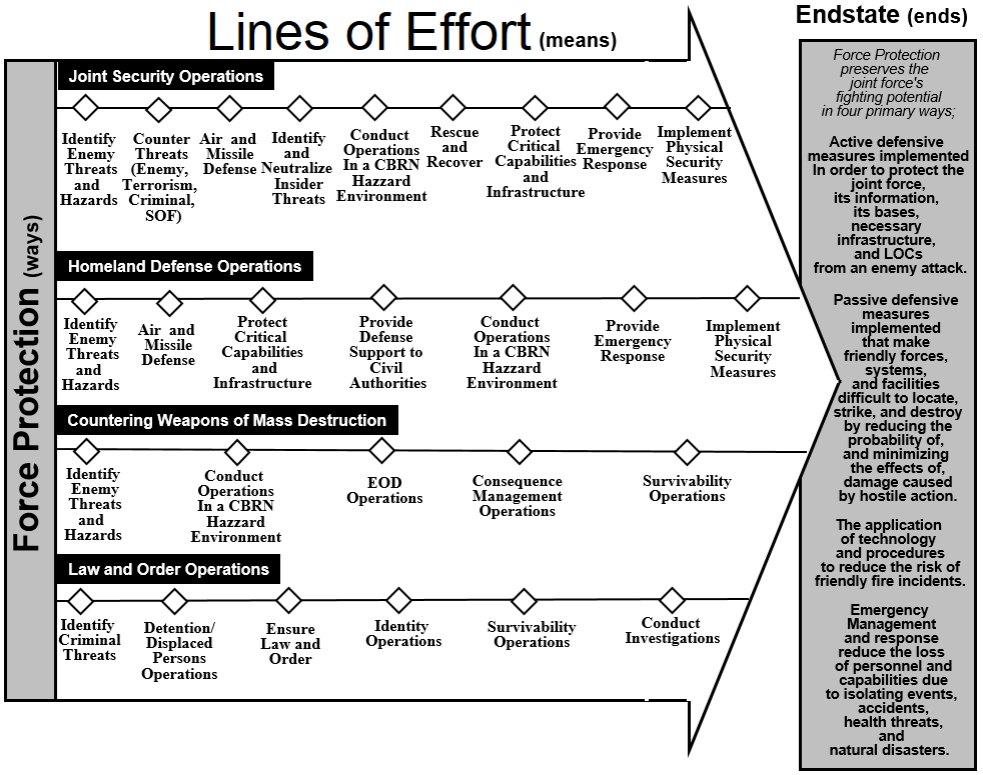
MARFORPAC Force Protection Policy
- New Publication
- In Draft (OPR, MFP Force Protection)

MCO 3440.0, Marine Corps Emergency Management Program
- Cancels and replaces MCO 3440.9
- **Currently out for FO/GO Review**

MARPFORPAC CBRND Program
- New Order
- **Currently out for signature**

MARFORPAC Physical Security Program
- New Order
- **Signed/Published 26 July 2021**

MARFORPAC Mass Warning Notification System Policy
- Cancels and replaces interim policy, MFP Policy 02-15
- **Currently out for O-6 Level Review**



Joint Intermediate Force Capabilities

Intermediate Force Capabilities

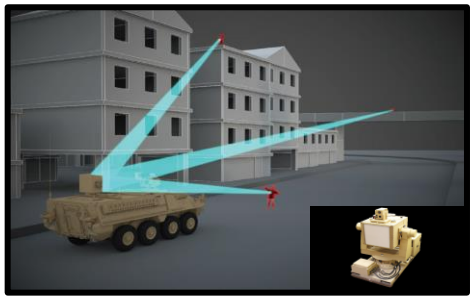
Active Denial Technology (ADT) is a non-lethal, counter-personnel, directed energy (DE) Intermediate Force Capability (IFC) that creates a heating sensation, quickly repelling potential adversaries. ADT provides the Joint Force with an option to stop, deter, and turn back suspicious individuals with minimal risk of injury or damage to critical infrastructure.

Traveling at the speed of light, an invisible DE beam of radio frequency millimeter waves engages the subject, penetrating skin to a depth of 1/64th of an inch—the equivalent of three sheets of printer paper. This *repel* effect produces an intolerable heating sensation, compelling the targeted individual to instinctively move. It ceases immediately after the individual moves out of the beam or when the operator turns off the ADT system. There is minimal risk of injury due to the shallow energy penetration of the skin, normal human instinctive reactions, and system engineering controls.

Active Denial Technology systems produce reversible effects at distances up to and beyond small arms range, providing U.S. forces with additional decision time and space to validate that a perceived hostile intent/act is, in fact, hostile. ADT may be used to complement force application and force protection missions.

From 2002 to 2007, the Active Denial System (ADS) Advanced Concept Technology Demonstration produced two ADT systems: System One, integrated the technology with a High Mobility Multi-Purpose Wheeled Vehicle; System Two was built as an armored, containerized system transportable by tactical vehicles. Each successfully completed a series of land- and maritime-based military utility assessments. From 2014 to 2015, System One was refurbished into a more mobile system transportable by a Marine Corps Medium Tactical Vehicle Replacement truck. Both prototypes are long-range, large spot-sized systems suitable for testing, evaluation, exercises, and demonstrations. From 2010 to 2015, a more compact, shorter-range, solid-state technology-based ADS was built in partnership with the U.S. Army, and is also available for testing and evaluation.

System One



Solid State-ADT

Counter Insider Threat

Organizational Assistance

Resilience at the individual and organizational level are part of a tool-kit necessary to prevent personnel from going down a path that leads to negative outcomes. It is each person's responsibility to help themselves and others stay on track. This is achieved through **prevention**, **assistance**, and **response**.

Resilience

- Resilience is not a special trait or gift, it is the ability to bounce-back from difficult experiences.

Prevention, Assistance, and Response (PAR)

- The purpose of the PAR concept is to aid leaders in helping persons at risk for potentially violent behavior before these persons commit violent acts to themselves or other people.

Example Traits of Individual Resilience:

- Physical Fitness – a strong muscle system, cardiovascular system, and immune system prepares your heart and body for stressors.
- Sleep – improves decision making, decreases irritability, and increases energy.
- Metal Preparation – having a mental and physical rehearsal strategy to help you not only in Marine Corps tasks, but in life challenges as well.
- Cognitive Flexibility – ability to bend and not break when circumstances change, or things do not go according to plan.
- Social Connection – humans have an innate need for connection. Connect with those who provide support.
- Sense of purpose and commitment – the dedication to something bigger than yourself.

Example Traits of Organizational Resilience:

- Provide resources to all personnel – civilian, contractor, Marine, Sailor, and family member.
- Provide new personnel with the organization's mission statement – help new personnel learn where their efforts contribute to the mission.
- Connect with your personnel – rapport will increase the likelihood that they will communicate when there is a problem.
- Establish Credibility, trust, rapport, and buy-in from staff.

The Marine Corps is committed to protecting personnel and critical information while preserving privacy and civil liberties. Proactive Insider Threat reporting can deter, detect, and mitigate potential insider threats.

Antiterrorism Operations

As the Marine Corps transitions to become the Force as articulated by the 38th CMC Planning Guidance, commanders will be asked to think beyond the traditional low-level threats and hazards which have dominated USMC Antiterrorism Programs. Small units will be operating under decentralized C2 structures in climes and places that test our resolve. While much will be new to us, the Marine Corps Planning Process and our Risk Management Methodology will not change. More than ever, ATOs at all levels of command must ensure they are fully embedded within the commander's planning process to ensure risk is mitigated to acceptable levels.

Adversary Special Operation Forces (SOF)

Capabilities: Adversary SOF possess the ability to infiltrate undetected behind enemy lines and maintain a three-dimensional, all weather infiltration capability:

- Sea - submarine, high speed boat, surface swim, or SCUBA
- Air - parachute, and helicopter insertion
- Land – all terrain long-distance movement

Doctrine: Adversary SOF warfare doctrine consists primarily of special reconnaissance, attacks, sabotage, integrated land-sea-air-space-electronic combat, and surgical strikes.

Mitigation Tactics: The use of speed, mobility, and screening techniques with the passive and active fundamentals of defense should be used to mitigate the effectiveness of SOF

Passive Mitigation Measures:

- Sensors
- Obstacles
- Barriers
- Fighting positions
- Cover
- Concealment

Active Mitigation Measures:

- Patrolling
- OP/LP's
- Emissions control
- Deception
- Maneuver/ Mobility

Personnel Recovery

Personnel Recovery in WW II

During WW II rescue in the Pacific theater centered around two different types of recovery vehicles.

Aircraft in the form of the OS2U Kingfisher, a single engine floatplane, was capable of launching from ships such as Battleships and Cruisers. These aircraft could be recovered alongside the ships. The Kingfisher was used as opportunities arose. The PBY Catalina, a twin-engine amphibious aircraft was used for longer-range rescues. It became the dominate aircraft during the early years of 1941-1943. From 1943 onward, it became the main recovery SAR aircraft used by the US in Pacific theater.

Ships, both surface and subsurface were the other recovery platforms. Naval vessels could be pre-positioned along aircraft ingress and egress routes for rescue purposes. Smaller vessels such as PT boats were assigned to short-range missions. On longer missions, submarines were asked to stand by in the area in case airmen needed to bail out before returning home. This was the start of Life Guard Duty assignments.

The first time submarines performed lifeguard duty was during the bombing of Wake Island in December 1942. Although not needed during that mission, it was the start of a vital new mission for submarines during the war.

Did this Life Guard duty make a difference?
On Sept. 2, 1944, the USS Finback rescued LTJG George Herbert Walker Bush, future president of the United States.

Emergency Management

Hurricane/Typhoon Preparedness

The Pacific Hurricane season is from June 1st to November 30th. Ensure you and your family are prepared:

- ***Help is an ocean away!*** The Hawaii Emergency Management Agency recommends a 14-day emergency kit for each family member due to Hawaii's location in the Pacific. A disaster on Hawaii will require additional time for resources to be delivered compared to the mainland.

CBRN Defense (Operations)

The CBRN Defense section contributes to MARFORPAC Force Protection Readiness through a combination of Marine Air Ground Task Force (MAGTF) general purpose force (GPF) and specialized, low density skill sets residing within each Major Subordinate Command. Each Major Subordinate Command maintains the Dismounted, Reconnaissance, Sets, Kits, and Outfits (DRKSO) which provides a commander an enhanced reconnaissance and surveillance capability within the MAGTF.

Support to CWMD

In addition to the DRSKO, the Marine Corps maintains a high-resolution gas chromatography (GC) and mass spectrometer (MS) in a portable, ruggedized device. The GCMS can detect and provide field-confirmatory results of chemical warfare agents, explosives, drugs, and toxic industrial chemicals in gases, vapors, liquids, and solids. It can also identify trace compounds that can go undetected by other technologies. Field confirmatory results negates the need for theater lab analysis thus providing the commander quick information on current threats.

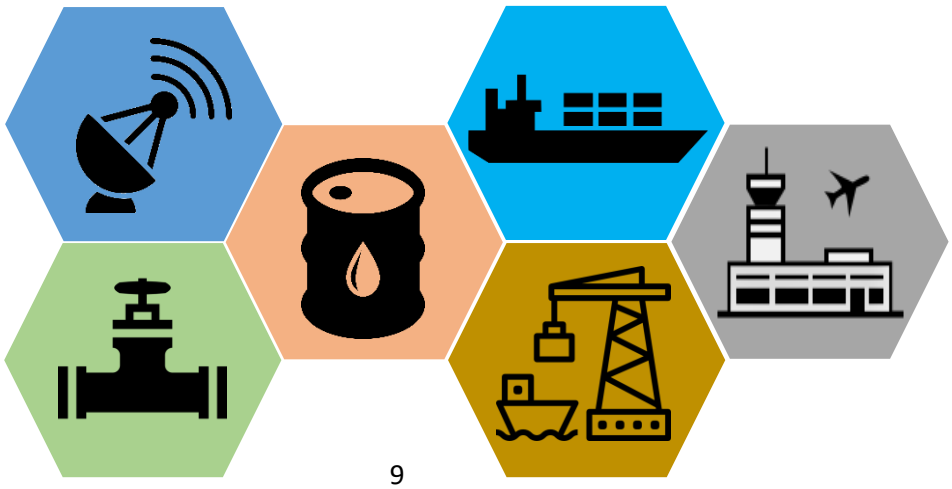
Critical Infrastructure Protection

"The United States is a society totally dependent on interlocking networks and nodes for communications, transportation, energy transmission, financial transactions, and essential government and public services. Disruption of key nodes by terrorists could cause havoc, untold expense, and perhaps even mass deaths. *"We are, in the jargon of the trade, a 'target-rich environment.'"* Senator Patrick Leahy, 1990.

The DoD represents a microcosm of the United States and depends heavily on "interlocking networks and nodes for communications, transportation, energy transmission" for mission success. Since Senator Leahy's remarks, the DoD has taken great strides to identify, prioritize, and validate infrastructures, assets and capabilities deemed critical to both joint and USMC operating forces in order to support their warfighting missions. We began with identifying critical assets and infrastructures and providing assurance through analysis, assessment, and remediation. The DoD's Critical Infrastructure Protection (CIP) Programs may also review the protection of some commercial assets and infrastructure services the DoD may rely upon. Other responsibilities for CIP included assessing the potential impact on military operations that would result from the loss or compromise of infrastructure service. Additionally, there are requirements for monitoring DoD operations, detecting and responding to infrastructure incidents, and providing department indications and warnings, all as part of a national process. Ultimately, CIP has assumed a vital responsibility for supporting national critical infrastructure protection.

On March 9, 1999, Deputy Defense Secretary John Hamre warned the United States Congress of a "electronic Pearl Harbor" saying, "It is not going to be against Navy ships sitting in a Navy shipyard. It is going to be against commercial infrastructure". Later that fear was qualified by President Clinton after reports of a series of actual cyber terrorist attacks in 2000.

In May 1998, presidential directive PDD-63 was issued by Bill Clinton. The directive documented areas of national infrastructure that were deemed critical to the national and economic security of the United States and the steps that were required to protect these areas. Today, the MARFORPAC Critical Infrastructure Protection program continues to support this directive in an effort to mitigate the effects of the potential loss or disruption of infrastructures, assets, and capabilities deemed critical to mission success.



Military Police Operations

Extension of MCBUL 5810 Criminal Justice Information Reporting Requirements and Guidance

Last month a federal judge ruled the U.S. Air Force is largely responsible for a 2017 mass shooting at a Texas church that killed 26 because it failed to report the shooter's criminal history to the FBI. "Had the Government done its job and properly reported Kelley's information into the background check system—it is more likely than not that Kelley would have been deterred from carrying out the Church shooting," U.S. District Judge Xavier Rodriguez for the Western District of Texas wrote in the court ruling.

In response to the 2017 shooting, the Marine Corps published MCBUL 5810 to establish policy on criminal justice information reporting, and this MCBUL was just extended by MARADMIN 372/21. **Yearly firearm purchase denials for USMC associated individuals has increased from 18 in 2018 to 123 in 2020, with 117 purchase denials in 2021 as of August.** The system is working, however:

Currently, approximately 30% of required reporting in the Marine Corps has not been completed. Commanders are required to submit offender disposition for arrests/apprehensions to supporting Law Enforcement Agencies within 5 business days.

Vignette 1: A PMO patrol observes two Marines fighting in front of the BEQ. Investigation reveals neither Marine has any injuries, and the assault was mutual. Both Marines are apprehended for assault, FBI criminal finger prints are taken and submitted, and the Marines are turned back over to their command. The command issues both Marines a 6105.
Required CJIS Reporting: The command must provide the PMO with the adjudication on the assault, the PMO must submit the adjudication to the FBI to close out the criminal incident reporting. If this follow up reporting does not take place by the command or the PMO, a criminal background check conducted by civilian law enforcement or any other agency, will show pending criminal charges for assault.

Vignette 2: A barracks duty NCO observes two Marines fighting in front of the BEQ, and breaks up the fight. The chain of command is notified, and both Marines receive a 6105.
Required CJIS Reporting: None. No law enforcement investigation was initiated, reporting for this offense is not covered by MCBUL 5810, enclosure (2).

Vignette 3: A Marine's random urinalysis comes back positive for a controlled substance, receives NJP and is process for administrative separation.
Required CJIS Reporting: The unit must coordinate with servicing law enforcement agency to conduct CJIS reporting as reporting is required by MCBUL 5810, enclosure (2). The Gun Control Act prohibits possession of a firearm. **The command and the Marine Corps could be liable for crimes committed with a fire arm that should have been barred from purchase.**

Physical Security

Notice:
Starting September 1, MARFORPAC Physical Security will be turning off and removing redundant card readers within restricted spaces. If there is still a need to lock spaces within restricted areas, sections will need to purchase locks and have them installed by facilities. For questions on how to purchase locks and their installation, contact GySgt Tidwell (S4) 477-8830.

Purpose

Plan for and implement active and passive physical security measures presenting a security profile commensurate with the threat in order to safeguard personnel, property, and equipment against unauthorized access, espionage, sabotage, wrongful destruction, malicious damage, theft/pilferage, and other acts which degrade mission readiness.

Restricted Areas

-Must have an Access Control Officer and a Responsible Officer (RO) assigned in writing.
-Must have an authorized access control letter of authorized personnel displayed on the inside of the door.
-Must have SF (702 & 703) Forms on the exterior of the door.

REMEMBER TO SPIN YOUR LOCKS IF YOU ARE THE LAST ONE LEAVING FOR THE DAY

Level One	Level Two	Level Three
Causes Damage	Causes Serious Damage	Causes Grave Damage

All Restricted areas must be designated in writing by the Commanding Officer and are required to undergo an annual Physical Security Survey.

Access Control

Access control is a vital part of any Physical Security Program. This requires all personnel within an organization to do their part.

Piggy backing:
Piggy backing occurs when an authorized individual permits others to follow behind without showing or registering proper authorization and gains access to a secure area.

Tailgating:
Tailgating occurs when an individual gains access by exploiting poor situational awareness of an authorized person.

To report a lost item please send an email to **MCBH_PHYSICAL_SECURITY@usmc.mil** or call **808-257-8559**.

Explosive Ordnance Disposal

Very Important Persons Protection Support Activity (VIPPSA)

The DOD has been providing EOD support to the U.S. Secret Service (USSS) and Department of State (DOS) on a recurring basis since 1958. This support involves protection of the President of the United States (POTUS), the Vice President of the United States (VPOTUS), Secretary of State (SECSTATE) and other U.S. and foreign dignitaries that require VIP protection. DOD Directive 3025.13 (Employment of DOD Capabilities in support of USSS) assigns USNORTHCOM / Joint EOD Very Important Persons Protection Support Activity (VIPPSA) as the DOD OPR for routine (25 or fewer EOD teams) support. The CJCS Standing ExOrd directs the services and CCDRs to provide support on a recurring basis.

Support requests are generated from the USSS or DOS and sent to VIPPSA who then task the services and/or CCDRs to support. The Marine Corps Watch Office and HQMC (LPE) receives the task from VIPPSA then, LPE forwards the task to MARFORPAC, MARFORCOM and/or MCICOM. The MARFOR's will further forward the task down to the MEF and from MEF to each respective chain of command for each EOD unit.

The MARFORPAC EOD Officer coordinates VIPPSA tasks requiring EOD support to available MEF units owning EOD assets through availability reporting and prior coordination with the MEFs IAW MCO 3571.2H (EOD Program). This coordination has been and is extremely vital due to inherent immediate support requirements that may arise with as little as 24 hour notice.

Information Protection

Information Protection encompasses the Information, Personnel, and Industrial Security Program requirements and policies for the protection, handling and safeguarding of Controlled Unclassified Information, and Classified National Security Information (NSI) (Top Secret and below) throughout its lifecycle.

Last month introduced a few key concepts of the Information Security Program.

This month will discuss proper handling and safeguarding of Classified Material.

ALL CLASSIFIED MATERIAL MUST BE PROPERLY SECURED IN A GSA CONTAINER
WHEN NOT IN USE OR IN THE DIRECT CONTROL OF A CLEARED INDIVIDUAL WITH NEED-TO-KNOW

- Going to the restroom – Secure your classified
- Going to the MCX Marine Mart – Secure your classified
- Going to the gym – Secure your classified
- Going to lunch – Secure your classified
- Going to a meeting – Secure your classified
- Going home - Secure your classified

Classified matterial cannot be stored with:

- Weapons (guns/ammo)
- Funds (money/jewelry)
- Drugs

Individuals will be held accountable for the proper handling, marking, and safeguarding of all classified material that they have been entrusted with.

Penalties for violating improperly handling, marking, safeguarding or storing classified material range from civil and criminal penalties under applicable Federal laws, the UCMS, as well as administrative sanctions.

Please copy and paste the below link in to your browser to read about what can happen if you fail comply with security requirements for the protection, handling, safeguarding and storage of classified material.

https://breaking911.com/executive-assistant-to-the-u-s-indo-pacific-command-admits-to-stealing-classified-secret-material/

Foreign Disclosure

If you have a requirement to release/disclose information to a foreign government or international organization, then the product requires review for disclosure/release.

Foreign Disclosure Officers (FDO) will ensure a judicious decision is made considering the disclosure/release of the request, while providing clear and well-reasoned analysis, guidance, and recommendations.

FDMS is a portal designed for requestors to submit products for a disclosure review with the intention of sharing this information with partner nations or international organizations. FDMS serves as a central repository and stores all submissions for future retrieval IAW DoD Directive 5230.11, SECNAVINST 5510.34B, and MCO 5510.20C. The submitter sees products they have submitted and once a release determination has been made by the FDO, the submitter receives an email notification of the approval, which contains a link to the determination.

FDMS will prompt the requestor to submit the given product as well as information pertaining to that product. Before creating a submission, consider the following:

- What is the benefit to the U.S.?
- What are the security risks associated with the disclosure?
- How will the product be shared? (oral, visual, or documentary)
- Who is the intended audience?
- What is the venue for the disclosure?
- Who is the proponent for the product?
- Has the product already been approved for disclosure to the proposed audience? If yes, has anything been changed?
- Is the information deemed to already be in the public domain? For example, was the information placed on a public facing website by the authorized proponent?
- Are the proper classification markings are on each bullet, picture, maps and graphics?
- On photos, has credit for the photographer been noted?

Decisions: There are three decisions the FDO may reach: approval of the submitted product, approval of a *sanitized* version of the product, or disapproval of the product.

Response Times: The requestors should allow enough lead time for a decision. As MARFORPAC does not have Original Classification Authority (OCA) most cases will require consent from another service or command who owns the information/product. The owners/originators of the information will need to grant MARFORPAC consent to release/disclose their information. In most cases, FDOs must receive the product a minimum of 10 working days prior to intended release. Due to operational tempo and short notices, this may not be an option. In this situation as much time as possible is requested.

**FDO's use the originator/source documents in the review process.

FDMS site (NIPR):
https://intelshare.intelink.gov/sites/marforpac/Sections/Security/Pages/FDMS_Dashboard.aspx

Contact Information

Organizational Email:
marforpac.forcepro@usmc.mil

Force Protection Officer/ Branch Head
Brian Whalen
808 477-8618
brian.j.whalen1@usmc.mil

Explosive Ordnance Disposal Officer/Deputy Branch Head
LtCol Daniel Cusinato
808 477-8457
Daniel.cusinato@usmc.mil

CBRN-D SNCO/Branch Chief
MGySgt Kierre Campbell
808 477-8673
kierre.campbell@usmc.mil

Joint Intermediate Force Capabilities
Barclay Lewis
808 477-8920
barclay.lewis.ctr@usmc.mil

Antiterrorism Operations
Rob Norton
808 477-8718
robert.norton@usmc.mil

Mike Andrews
808 477-8635
michael.j.andrews@usmc.mil

Personnel Recovery/ Foreign Disclosure Officer
Kevin Keenan
808 477-8923
kevin.keenan@usmc.mil

CBRN-Defense
CWO5 Brian Barksdale
808 477-5818
brian.barksdale@usmc.mil

MGySgt Kierre Campbell
808 477-8673
kierre.campbell@usmc.mil

Mike Bender
808 477-8380
michael.a.bender@usmc.mil

Critical Infrastructure Protection
Brian Nuss
808 477-8950
brian.nuss@usmc.mil

Military Police Officer/ Counter Insider Threat/ Emergency Management
Maj Kris Knobel
808 477-8930
kristopher.knobel@usmc.mil

Physical Security
GySgt Keily Warren
808 477-1846
keily.warren@usmc.mil
marforpac.physec@usmc.mil

Information Protection
Command Security Manager
Brian Chun-Ming
808-477-8704
brian.chunming@usmc.mil

Imminent Threats
Call 9-1-1!